PRIVACY IMPACT ASSESSMENT (PIA)

For the

Identity Management (IDM)
Defense Information Systems Agency (DISA) - Computing Services Directorate (CSD)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☒	**New DoD Information System**	☐	**New Electronic Collection**
☐	**Existing DoD Information System**	☐	**Existing Electronic Collection**
☐	**Significantly Modified DoD Information System**		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒	**Yes, DITPR**	Enter DITPR System Identification Number	11682
☐	**Yes, SIPRNET**	Enter SIPRNET Identification Number	
☐	**No**		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☐ **Yes** ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier K890.12

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date. 1/12/2010

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

The authority allows IDM to collect the following data:

Authority for maintenance of the system: a5 U.S.C. 301, Departmental Regulation; 10 U.S.C. chp 8; DoD Directive 5105.19, Defense Information Systems Agency (DISA); E.O. 9397 (SSN)

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:
The 'Blanket Routine Uses' set forth at the beginning of the DISA's compilation of systems of records notices apply to this system.

DISA's rules for accessing records, for contesting contents and appealing initial agency determinations are published in DISA Instruction 210-225-2 at 32 CFR part 316 or may be obtained from the system manager.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

Identity Management (IDM), will provide centralization of cross platform system account and user identity management. This functionality will include account provisioning, password synchronization and centralization of system access management. The solution provides a standardized web based work flow for the current SAAR (DD2875) process.

The system will store PII information that can be found on the current DD2875 form. This PII information is as follows: Full Name; Job Title/Grade/Rank; Citizenship; Social Security Number (SSN); and Clearance Level.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The privacy risks associated with the PII collected are the unauthorized release of PII data. These risks are addressed by encrypting the data in compliance with the FIPS 140-2 requirement for storing Social Security Numbers (SSN), by using strong SSL encryption with Common Access Card (CAC) authentication under the routine use guidelines authorized in the Privacy Act SORN, and through periodic Information Assurance certification of personnel with access to the PII.

The Buildings in which the servers are housed are secured by guards during duty and non-duty hours. Access to records is controlled by management personnel, who are responsible for maintaining the confidentiality of the records and using the information contained therein only for official purposes. Access to PII is restricted to those who require the records in the performance of their official duties.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. Personnel responsible for processing correspondence containing PII.

☒ **Other DoD Components.**

Specify. All DoD Components that have equity in a specific action containing PII.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. **Do individuals have the opportunity to object to the collection of their PII?**

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Disclosure of information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of the request.

(2) If "No," state the reason why individuals cannot object.

j. **Do individuals have the opportunity to consent to the specific uses of their PII?**

☐ **Yes** ☒ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

DoD employees (military and civilian) cannot give or withhold consent since the purpose of IDM is to provide system access authorization and track system/application users that are utilizing DoD systems/applications that may house sensitive information.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒	**Privacy Act Statement**	☐	**Privacy Advisory**
☐	**Other**	☐	**None**

Describe each applicable format.

The System Authorization Access Request System provides Privacy Act Statement to collect PII data;

Authority: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse and Act.

Principle Purpose: To record names, signatures, and Social Security Numbers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense systems and information. NOTE: Records may be maintained in both electronic and/or paper form.

Routine Uses: None.

Disclosure: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.